An Open Call for Security and Privacy Researchers to Resist Back Doors

Abstract

This document serves as a call to action for security and privacy researchers to resist back doors and protect the security and privacy of the individual and the nation. It starts by providing a brief overview of the technical details surrounding this issue and informally modeling the threat introduced by back doors. Next, the document provides a background on the legal aspects of the debate through the lens of three major landmark cases and laws. It then details the opinions of various government agencies on the back door problem. Finally, the document lays out a plan of action that security and privacy professionals can follow to take a more active role in shaping the future of this debate.

Introduction

Law enforcement such as the FBI and local police authorities have long been able to easily perform digital forensics on suspects' personal computers and mobile phones. They have also been able to wiretap the suspects' communications and request information about their usage from telecommunications companies. However, the widespread adoption and implementation of encryption technology has made law enforcement's job significantly more challenging. Now, they are calling for laws that require companies to install back doors to get around security protections and make investigations much easier. As the security and privacy community, we know that these back doors are intentionally making our systems more vulnerable which would do way more harm than good. We need to push back against these laws by engaging with lawmakers and educating them on the dangers of back doors and benefits of encryption. We can do this by educating ourselves on the arguments made by the opposition, writing letters to politicians' offices detailing our views on back doors, and speaking in legislative hearings at local, state, and federal levels. The security and privacy community has not been outspoken enough, and this proposal seeks to provide it with a plan of action.

Landscape of Issue

From a technical perspective, allowing the government to plant back doors requires users to place trust, in the technical sense, in the government. Best security practices say you should establish trust in the recipient and as few others as possible. On a single device, this involves trusting just yourself, since the key is stored on the device and never shared assuming only you know the password. Introducing a back door would require trust to be placed in the person using the back door. All this assumes that the only person with access to the back door is the government. Given how skilled other nation-state threat actors are at reverse engineering, this seems like an overly optimistic assumption to make. In this scenario, you are placing trust in some very malicious actors. This is much like the baggage locks approved by the Transportation Security Administration (TSA). The TSA wanted to ban baggage locks to make security screening in airports easier and quicker. This caused much uproar because travelers wished to lock their bags to prevent theft. As a compromise, the TSA released approved locks that they have skeleton keys to open. This quickly backfired because people were able to reverse engineer the locks and create keys that could open all TSA approved locks [1]. All travelers who use the approved locks are placing trust not only in the TSA, but in anyone in the airport who has recreated the key.

Legal Background

The legal aspect of the back door issue has been shaped by a few key laws and cases. The first is the Wiretap Act. This law was originally passed in 1968 but was amended in 1986. It allows law enforcement to request an order which authorizes them to intercept all wire or oral communications of a specified person. If the order (subpoena) is granted, the Wiretap Act allows the holder to request full access to "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively" [2]. When the law was first passed, its reach was limited to only wire and oral communication. However, when it was amended in 1986 the scope was expanded to include electronic communications. Some argue that the Wiretap Act as currently constructed can be used to force back doors into software [2]. The modification of the service could be portrayed as technical assistance which is covered by the law. This may not have been the intention of the law, but legal experts warn that the language is vague enough to be taken advantage of [2]. In order to maintain and improve security going forward, we need to ensure that the wording of these laws is as clear as possible so that they cannot be manipulated in any way. Much like how an attacker will exploit any small flaw to gain access to a system, law enforcement will use any vague language to justify forcing the installation of back doors.

United States v. New York Telephone Co. in 1977 was the second landmark case in the legal discussion around government and law enforcement back doors. This case revolves around the power granted by the All Writs Act which grants the courts the ability to "issue all writs necessary or appropriate in aid of their respective jurisdiction" [2]. The FBI received approval from a District Court to install a pen register, which is a device that logs the phone numbers dialed by a certain device. The court order also required the New York Telephone Company to cooperate fully with the FBI to install the pen registers. The Telephone Company argued that they were not required to assist the FBI and that only a request made under the provisions of the Wiretap Act could force assistance. The Court of Appeals sided with the Telephone Company, but the Supreme Court claimed that the All Writs Act granted the District Court the authority to force the Company to comply. This decision sets a precedent that companies are required to help law enforcement when it is deemed to require minimal effort [2]. The danger is that the phrase "minimal effort" is not defined very well and could be used to force many companies to install back doors. The primary flaw with this case and the All Writs Act is that "minimal effort" is left up to interpretation. Law enforcement will only ever interpret this phrase in a way that allows them to force cooperation with orders for back doors. By working with politicians, we can help ensure the new legislation is clear-cut and does not allow this level of flexibility, which in turn improves overall security.

The third key legal factor is the Foreign Intelligence Surveillance Act (FISA). The act allows the Attorney General and the Director of National Intelligence to create written requests that require service providers to "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition" [2]. This provides the federal government much of the same vaguely worded power as the Wiretap Act, but with one key difference: the service provider must comply with the order in secret. Requiring the provider to assist in secret makes it very difficult for the general public to know if their privacy is being violated [2]. The original intention for FISA was to allow the government to more effectively gather intelligence on foreign targets and threats, but it is clear that the government can secretly issue requests for back doors under FISA [2]. Some may argue that these are harmless since the special access is kept hidden, however, as security professionals, we recognize this thinking as security by obscurity and know that it actually weakens the system. This is something we need to emphasize to legislators, so they see how back doors are actually harmful to the security of both the individual and the nation.

Other Groups' Opinions

When discussing the battle against back doors, many security professionals tend to assume that the two groups at odds are the security community and the government. However, this is not the case. There are many different branches of the government that are in favor of strong encryption and maximum digital security. These groups depend very heavily on the ability to send data that is unreadable by third parties and is not modified in flight. One such group is the United States Department of Defense. When speaking at the RSA Security Conference in 2016, Former Secretary of Defense Ashton B. Carter said he didn't support a back door that would give the government unfettered access to encrypted data [3]. He specifically said that he was "not a believer in back doors or a single technical approach." Former Secretary Carter went on to say he did not think back doors were a "realistic" or "technically accurate" solution to the surveillance problem [3]. Later that year at a press conference, he said, "we know that strong encryption is part of the solution for the future" [4].

At this same press conference, Former Secretary of Commerce Penny Pritzker echoed Carter's sentiments by stating, "It's extremely important we have strong encryption" [4]. She justified her belief by explaining that "our entire economy rests on the back of the digital infrastructure" [4]. Former Secretaries Carter and Pritzker were some of the highest-ranking officials in the US government, and it is reasonable to believe their opinions reflect the mindset of the departments they head. These quotes make it very clear that the Departments of Commerce and Defense rely on encryption to effectively carry out their duties and are opposed to installing back doors that would compromise encryption. It is clear now that our battle is not against the entire US government, but only certain parts of it. We have to focus our efforts specifically towards the parts that are in favor of back doors.

As we know, the Federal Bureau of Investigation (FBI) is the most vocal supporter of back doors in the government. Strong encryption makes digital forensics much more difficult, and as a result the FBI is the branch of the government most negatively impacted by strong encryption. Due to this, it makes sense that they are the ones most often calling for weaker encryption and security standards. James Comey, Former Director of the FBI, said that there is a large number of devices that have data they cannot obtain access to due to the encryption [4]. To highlight the complexity of the issue, Comey said, "I love strong encryption. Encryption is a very, very good thing. I also love public safety" [4]. He described how the two are currently at odds and that there needs to be more discussion on the balance between individual privacy and public safety. Former Director Comey's statements accurately depict the issue as multi-faceted rather than just black and white. More importantly, it shows that the FBI is not totally against encryption and understands its value. Instead, they express a willingness to have open dialogue to work towards a solution that benefits everyone. Rather than depict groups like the FBI and other law enforcement as the villains, we have to work with them in order to create technical solutions that provide privacy and hep law enforcement do its job.

Plan of Action

In order to effectively change law enforcement and lawmakers' opinions on back doors, we first need to understand why they feel the back doors are necessary. This can be done by looking into each lawmaker's policies in this area and reading about their beliefs on technology policy. We also need to examine how they voted on bills that cover similarly technical topics such as net neutrality. This research will also help uncover any politicians who support strong encryption and are against back doors. These politicians can become great points of contact for starting the conversation going forward. Conducting research on the law enforcement opinion towards back doors will help put the whole back door issue into perspective. They claim that it makes their job of investigating crimes more difficult. Law enforcement also says that encryption helps criminals and terrorists hide their illicit activity and conversations. Diving into the technical details of what processes law enforcement uses will not only help guide constructive discussion but will help clarify the difficulties that need to be addressed with new technical solutions as well.

Once we understand the opposition's perspective, we need to write letters to the politicians' offices in order to get the conversation started. Many politicians do not know who the experts in the security and privacy fields are, so we need to take it upon ourselves to represent the fields. This includes contacting politicians on both sides of the back door issue. The best way to initiate this contact is to reach out to their offices and write letters to them. For many lawmakers writing letters to their offices is the most effective way of reaching them. In these letters, we have to introduce ourselves and establish our credibility as security and privacy experts. Next, we have to briefly explain our perspective on the back door issue. Finally, we should offer to engage more in any discussion regarding this issue. This will help make us known as the security technical experts so that the lawmakers can reach out to us when they are discussing this issue and need an expert's opinion. As Former Secretary of Defense Carter said at a conference, "[Laws] written in anger or grief… [are] not likely to work" [3].

Once we have the communication channel open, we have to volunteer to speak at hearings in order to broaden our reach to other politicians. Federal, state, and local governments all can hold hearings about these types of issues, and the best way we can create a strong impact is by casting a wide net. We have to reach out to politicians and lawmakers at all levels in order to participate in as many different hearings as possible. The House Homeland Security Chairman Michael McCaul and the Senate Intelligence Committee Vice Chair Mark Warner both agree that there needs to be a national commission to study problems like encryption [4]. These are the types of events that we need to organize and participate in going forward. When speaking at these events, we need to be very clear about how we are presenting the ideas about back doors. We have to make bold, clear claims. Many of the ideas that are recognized within the security field as universally true may be unknown by outsiders. One excellent example of this is in the Congressional testimony by Daniel Weitzner, Director of MIT's Internet Policy Research Initiative. In his prepared remarks, he boldly claims, "even those who are most sympathetic to law enforcement needs are joining the consensus that infrastructure-wide back doors are too risky to implement" [5]. This type of direct language is the most effective and efficient way to convey our field's beliefs to lawmakers because it leaves no room for misunderstanding. Dr. Weitzner goes on to explain the research that led to that conclusion but leading with the conclusion is a great way to frame ideas and make them clear.

Conclusion

As more technology companies enable encryption on their services and devices, law enforcement will continue to struggle to successfully perform forensics and wiretapping on suspects. Law enforcement will become more and more vocal about the need for back doors and legislators will feel pressure to pass laws which give them the power to request back doors. As the security and privacy experts, it is our responsibility to guide politicians to pass laws that support encryption and other best practices. We must ensure that we are taking a more active role in this conversation.

Works Cited

[1] I. J. McCarthy, “iOS Fear the Government: Closing the Back Door on Governmental Access,” *University of Toledo Law Review*, vol. 49, no. 1, pp. 179–201.

[2] C. Soghoian, “Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era,” *Journal on Telecommunications & High Technology Law*, vol. 8, no. 2, pp. 359–424, 2010.

[3] N. Perlroth, “Defense Secretary Says He's Not in Favor of a Data ‘Back Door’,” *New York Times*, 03-Mar-2016.

[4] Y. Tadjdeh, “Government Officials Conflicted about Encryption,” National Defense, pp. 28–29, 01-Aug-2016.

[5] United States. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations *Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives: hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, House of Representatives, One Hundred Fourteenth Congress, second session*. April 19, 2016.